A METHOD OF IMPLEMENTING ONE-TO-ONE BINARY FUNCTION AND RELATIVE HARDWARE DEVICE, ESPECIALLY FOR A RIJNDAEL S-BOX

Abstract of the Disclosure

A method for implementing one-to-one binary functions defined on the Galois field GF(2^8) is very useful for forming fast and low power hardware devices regardless of the binary function. The method includes decoding an input byte for generating at least one bit string that contains only one active bit, and logically combining the bits of the bit string according to the binary function for generating a 256-bit string representing a corresponding output byte. The 256-bit string is then encoded in a byte for obtaining the output byte.